PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-124955
(43)Date of publication of application : 28.04.2000

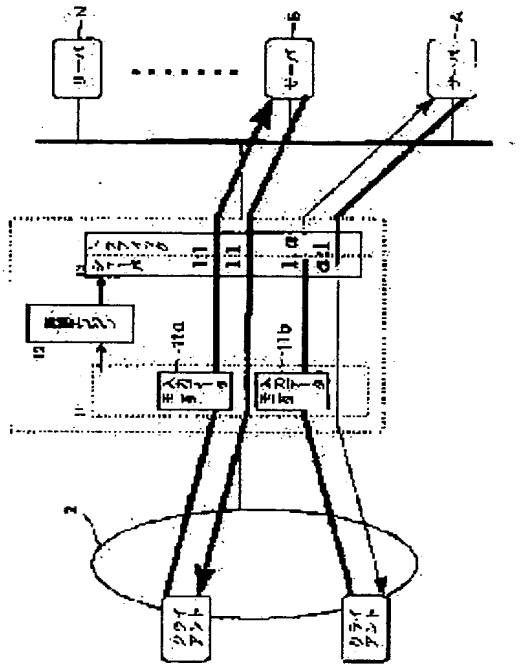
(51)Int.CI. H04L 12/56
H04L 12/40
// H04K 3/00

(21)Application number : 10-296522
(22)Date of filing : 19.10.1998

(71)Applicant : NEC CORP
(72)Inventor : HASHIMOTO JUNJI

(54) NETWORK ATTACK PROTECTION SYSTEM FOR TRAFFIC SHAPING

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a network attack protection system which can be effective to the attack by a scanner attacking totally, can unnecessitate the change of a server program and can quickly respond to the contents of the attack.
SOLUTION: Communication data transmitted from an external network 2 are sampled by input data monitors 11a and 11b. When an inference engine 12 detects matching between the pattern of communication data sampled by these input data monitors 11a and 11b and an attack pattern stored in the inference engine 12, the rate α of shaping traffic with a traffic shaper 3 is controlled.



LEGAL STATUS

[Date of request for examination]	19.10.1998
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3309961
[Date of registration]	24.05.2002
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－124955
（P2000－124955A）
(43)公開日　平成12年４月28日(2000.4.28)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｅ	５Ｊ１０４
12/40		Ｈ０４Ｋ　3/00		５Ｋ０３０
// Ｈ０４Ｋ　3/00		Ｈ０４Ｌ　11/00	３２０	５Ｋ０３２

審査請求　有　　請求項の数５　ＯＬ　（全　５　頁）

(21)出願番号　特願平10－296522

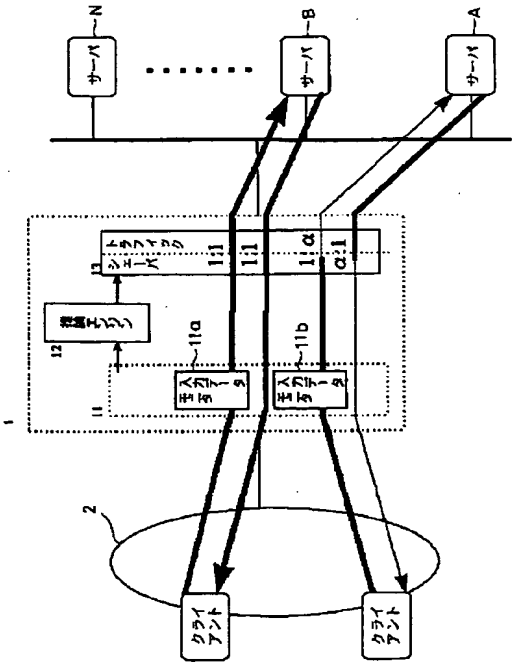
(22)出願日　平成10年10月19日(1998.10.19)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　橋本　淳二
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100089875
弁理士　野田　茂

Ｆターム(参考)　5J104 AA12 AA41 PA07
5K030 GA15 HC01 HC14 LC02 LC11
5K032 AA08 CC05 EA06

(54)【発明の名称】　トラフィックシェーピングによるネットワークアタック防御システム

(57)【要約】
【課題】　網羅的にアタックをかけるスキャナなどの攻撃に有効、かつサーバプログラムの変更を不要にでき、アタックの内容に即応できるトラフィックシェーピングによるネットワークアタック防御システムを提供すること。
【解決手段】　入力データモニタ１１ａ，１１ｂにより外部ネットワーク２から伝送される通信データを採取する。この入力データモニタ１１ａ，１１ｂで採取した通信データのパターンと推論エンジン１２に記憶されているアタックパターンとがマッチングしていることを推論エンジン１２で検出すると、トラフィックシェーパ１３によりトラフィックをシェーピングする割合αを制御する。



【特許請求の範囲】

【請求項１】　外部ネットワークからの通信データを採取する入力データモニタと、
コンピュータへのアタックパターンがあらかじめ記憶され、上記入力データモニタより採取された上記通信データのパターンを検出して、その検出した上記通信データのパターンが上記記憶したアタックパターンとのマッチングの有無により上記通信データが上記コンピュータへのアタックであるか、否かの判断をする推論エンジンと、
上記推論エンジンが上記通信データのパターンから上記コンピュータへのアタックパターン検出時にトラフィックをシェーピングする割合を制御するトラフィックシェーパと、
を備えることを特徴とするトラフィックシェーピングによるネットワークアタック防御システム。

【請求項２】　上記トラフィックシェーパは、上記推論エンジンによる上記通信データのパターンと上記アタックパターンのマッチング検出時にトラフィックをシェーピングする割合αを既定値（０＜α＜１）とすることを特徴とする請求項１記載のトラフィックシェーピングによるネットワークアタック防御システム。

【請求項3】　上記トラフィックシェーパは、上記推論エンジンによる上記通信データのパターンと上記アタックパターンのマッチング検出時にクライアントからサーバへのデータをα倍にすることを特徴とする請求項１記載のトラフィックシェーピングによるネットワークアタック防御システム。

【請求項４】　上記トラフィックシェーパは、上記推論エンジンによる上記通信データのパターンと上記アタックパターンのマッチング検出時にサーバからクライアントへのトラフィック量をα倍にすることを特徴とする請求項１記載のトラフィックシェーピングによるネットワークアタック防御システム。

【請求項５】　上記トラフィックシェーパは、上記推論エンジンにより検出したアタックの発信元である上記通信データが終了するとトラフィックをシェーピングする割合αを元の既定値（０＜α＜１）に戻すことを特徴とする請求項１記載のトラフィックシェーピングによるネットワークアタック防御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、トラフィックのシェーピングを行い、次のホストコンピュータ（以下、ホストと略称する）へのアタックへの移行時間を引き延ばすことにより、他のホストへのアタック時間を引き延ばすことができ、ホストへのアタックの解析が可能になり、アタックする犯人を特定するための情報を得ることができるようにしたトラフィックシェーピングによるネットワークアタック防御システムに関する。

【０００２】

【従来の技術】インターネットなどのパブリックネットワークの普及に伴い、ネットワーク経由による情報の盗難や不正利用などの犯罪が急増している。インターネットでは、不正アクセスのためのプログラムが流通しており、網羅的にアタックし、セキュリティホールを発見しようとするツールが数多く存在する。現在、これらのアタッキングツールやアタッカへの対策が急務であり、その対策に種々の試みがなされている。

【０００３】たとえば、特開平０２—３０２１３９号公報には、複数のネットワーク間の接続部に通信データの発信先アドレスと発信元アドレスをチェックし、アクセス権を記録した内容にしたがって、不正アクセスを遮断する不正アクセス防止手段を備えたネットワークセキュリティが開示されている。

【０００４】また、ＬＡＮあるいは公衆網などの伝送媒体に構築されるネットワークシステムにおいて、管理装置がアラーム情報と各中継装置が有するアクセス履歴情報とから不正アクセスをした端末装置が各中継装置のどちら側のポートに接続されているかを絞り込んでいくことにより、不正アクセスをした端末装置がどのＬＡＮ上で接続されているかを特定するセキュリティ方式が開示されている。

【０００５】

【発明が解決しようとする課題】しかしながら、これらの公報の場合には、いずれもホストへのアタックに対する直接的な対策とはならない。このような従来のネットワークアタック防御システムの課題を挙げると、以下のごとくである

【０００６】すなわち、従来は網羅的にインターネット上のサーバに対して「ポートスキャン」などを行われた場合、パケットフィルタリングなどにより、これらのアクセスを「遮断する」アイデアは存在した。しかし、この場合、アクセスを遮断することは即座に次のアタックに切り替わるきっかけとなってしまうことが多いため、アタッカは短時間でサービスポートなどを検出することができ、かつ迅速に次のアタックへ移行することができてしまうという課題がある。

【０００７】また、従来のアタックを遮断する方法もあるが、この方法では、攻撃元とのコネクションがすぐに切れてしまうことになり、攻撃元が次にどんなアタックを行うかを予想することが難しいという課題がある。

【０００８】この発明は、上記従来の課題を解決するためになされたもので、サーバ１台当たりのアタック時間を長くすることができ、網羅的にアタックをかけるスキャナなどの攻撃に有効かつ、サーバプログラムの変更を不要にでき、サーバに検出モジュールの導入を不要にできるとともに、アタックの内容に即した対応が可能となるトラフィックシェーピングによるネットワークアタック防御システムを提供することを目的とする。

【０００９】
【課題を解決するための手段】上記目的を達成するために、この発明によるトラフィックシェーピングによるネットワークアタック防御システムは、外部ネットワークからの通信データを採取する入力データモニタと、コンピュータへのアタックパターンがあらかじめ記憶され、上記入力データモニタより採取された上記通信データのパターンを検出して、その検出した上記通信データのパターンが上記記憶したアタックパターンとのマッチングの有無により上記通信データが上記コンピュータへのアタックであるか、否かの判断をする推論エンジンと、上記推論エンジンが上記通信データのパターンから上記コンピュータへのアタックパターン検出時にトラフィックをシェーピングする割合を制御するトラフィックシェーパとを備えることを特徴とする。
【００１０】この発明によれば、入力データモニタにより外部ネットワークから伝送される通信データを採取すると、この採集された通信データのパターンを推論エンジンにより検出される。検出された通信データのパターンが推論エンジンであらかじめ記憶されているコンピュータへのアタックパターンとのマッチングの有無を検出し、その検出の結果、アタックパターンと通信データのパターンがマッチングしていると判断すると、トラフィックシェーパにより、トラフィックをシェーピングする割合αを制御する。
【００１１】したがって、この発明では、サーバ１台当たりのアタック時間を長くすることができ、網羅的にアタックをかけるスキャナなどの攻撃に有効かつ、サーバプログラムの変更を不要にでき、サーバに検出モジュールの導入を不要にできるとともに、アタックの内容に即した対応が可能となる。
【００１２】
【発明の実施の形態】以下、この発明によるトラフィックシェーピングによるネットワークアタック防御システムの実施の形態について図面に基づき説明する。図１はこの発明の第１実施の形態の構成を示すブロック図である。この図１において、この第１実施の形態は防御装置１を備えている。クライアントＸ，ＹとコンピュータとしてのサーバＡ，Ｂ，・・Ｎには特別な仕組みは必要ない。
【００１３】防御装置１は、外部ネットワーク２からの通信データを採取する入力データモニタ１１ａ、入力データモニタ１１ｂによって得られた通信データのパターンを検出し、アタックかどうかを判断する推論エンジン１２と、トラフィックをシェーピングする割合を制御するトラフィックシェーパ１３とにより構成される。推論エンジン１２はあらかじめアタックパターンを記憶しており、推論エンジン１２により入力データモニタ１１ａ、入力データモニタ１１ｂによって検出された通信データのパターンとアタックパターンがマッチングしていることを検出することにより、アタックを検出する。トラフィックシェーパはアタック検出時にトラフィックをシェーピングする割合α（０＜α＜１）を記憶している。
【００１４】次に、以上のように構成されたこの第１実施の形態の動作について図２のフローチャート沿って説明する。図２のステップＳ１では、外部ネットワーク２を通してクライアントＸ、クライアントＹから伝送される通信データが入力データモニタ１１ａ，１１ｂによって採取される。この入力データモニタ１１ａ，１１ｂによって採取された通信データは推論エンジン１２で検出される。
【００１５】この推論エンジン１２には、あらかじめサーバＡ～Ｎへのアタックパターンが記憶されており、推論エンジン１２が入力データモニタ１１ａ，１１ｂによって採取された通信データを検出すると、その検出した通信データのパターンとアタックパターンとのマッチングの有無を検出する。この際、入力データモニタ１１ａ，１１ｂによって採取された通信データからアタックパターンらしい通信データが検出されるまで上ステップＳ１の処理の実行を繰り返す。
【００１６】推論エンジン１２は、入力データモニタ１１ａ，１１ｂによって採取された通信データの検出中に、この通信データのパターンがアタックパターンにマッチングすることを検出すると、ステップＳ２で推論エンジン１２はトラフィックシェーパ１３に対して、アタックパターンが検出されたことを通知する。トラフィックシェーパ１３は、この通知を受けると、トラフィックをα倍にシェーピングする。
【００１７】このシェーピングする状態は、図１におけるクライアントＹからサーバＡへのアクセスがこれに当たる。このトラフィックシェーパ１３はクライアントＹからサーバＡへの通信データを「１：１」から「１：α」倍に、また同様にサーバＡからクライアントＹへのトラフィックを「１：α」から「α：１」倍にする。推論エンジン１２により検出されたトラフィックが継続している場合であることをステップＳ３で推論エンジン１２が検出すると、ステップＳ４でトラフィックシェーパ１３はトラフィックの割合を減少するか、否かの判断を行い、トラフィックシェーパ１３はトラフィックの割合を減少させない場合には、再びステップＳ３の処理に戻る。
【００１８】また、ステップＳ４において、トラフィックシェーパ１３はトラフィックの割合を変更する場合（減少させる場合）には、ステップＳ５において、既定のトラフィックの割合（０＜α＜１）を変更して、ステップＳ２の処理に戻る。一方、上記ステップＳ３において、推論エンジン１２は検出したアタックの発信元からの通信データが終了したことを検出すると、ステップＳ６で推論エンジン１２はトラフィックのシェーピングを

既定値（０＜α＜１）に戻す。

【００１９】

【発明の効果】以上のように、この発明によれば、通信データとあらかじめ推論エンジンに記憶されたアタックパターンとの一致の検出時に、トラフィックシェーピングによってアタックのトラフィックを減少させるようにしたので、コネクションの保持時間を長くし、サーバ１台あたりのアタック時間を増加させることができ、１台あたりのアタック時間を増加させることは、網羅的にアタックをかけるスキャナなどの攻撃に有効である。また、サーバプログラムを変更する必要がなくなり、一個所で集中的にアタックの検出を行うため、それぞれのサーバに検出モジュールを導入する必要がなくなる。さらに、シェーピングによる時間稼ぎを行うことで、サーバのログから時間的余裕を持ってアタックの内容を見ることができ、これにより、アタックの内容に即した対応が可能となる。

【図面の簡単な説明】

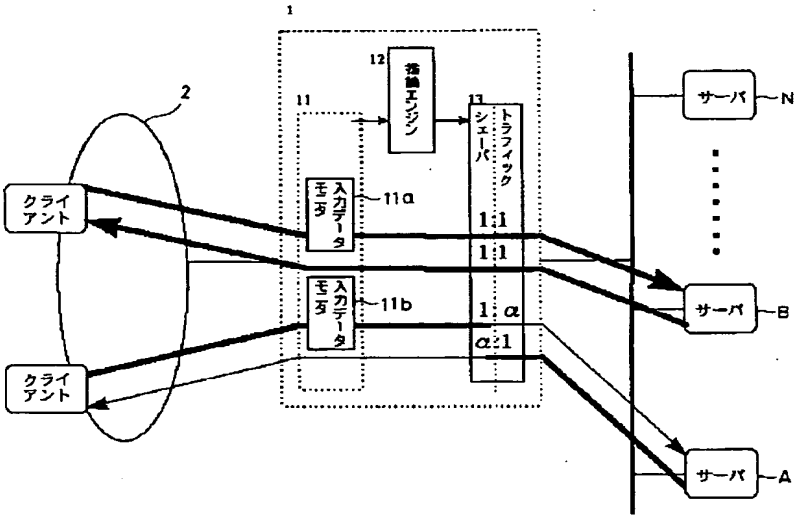
【図１】この発明によるトラフィックシェーピングによるネットワークアタック防御システムに第１実施の形態の構成を示すブロック図である。

【図２】図１のトラフィックシェーピングによるネットワークアタック防御システムの動作を説明するためのフローチャートである。

【符号の説明】

１……防御装置、２……外部ネットワーク、１１ａ，１１ｂ……入力データモニタ、１２……推論エンジン、１３……トラフィックシェーパ、Ａ～Ｎ……サーバ、Ｘ，Ｙ……クライアント。

【図１】



【図２】